1. 3PAO Readiness Assessment Report (RAR) Preparation

1.1 3PAO RAR Splash Screen

Notes:

Transcript

Title
Welcome to the 3PAO Readiness Assessment Report (RAR) Preparation Course

Text
Select the Next button to begin.

Image
Image of FedRAMP logo
1.2 Course Navigation

Audio
<N/A>

Notes:

Transcript
Title
Course Features and Functions

Text
Select each icon to view the topics and learning objectives

Image
Screen capture of the course including the FedRAMP logo, Transcript and Menu tabs, Navigation buttons, and Resources button.

Audio
Let’s take a moment to familiarize ourselves with the features and functions of this course. To navigate the course, you may select the Back and Next buttons located at the bottom of the screen, or you may use the Menu tab located on the left side of the screen to select the screen you’d like to view. Use the Play and Pause buttons located at the bottom of the screen to start and stop the screen content. You may also select the Replay button to view the content again. Use the Transcript tab on the left side of the screen to read a detailed description of the screen elements including the image descriptions, screen text, and audio script. You may also access the Resources button at the top right corner of the screen to open additional course resources.
Menu (Slide Layer)

Transcript (Slide Layer)
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

Resources (Slide Layer)

Play/Pause (Slide Layer)
Replay (Slide Layer)

Back/Next (Slide Layer)
1.3 FedRAMP 3PAO Training Roadmap

Notes:

Transcript
Title
FedRAMP 3PAO Training Roadmap

Text
Here is where you are in your training. Select any of the map points to see where you’ve been and where you’re going.
This is seventh course in the 3PAO series, which focuses on Readiness Assessment Report (RAR) Preparation. This course provides a discussion on how the FedRAMP security requirements must align with a CSP’s system security capabilities before the CSP system can be approved as FedRAMP Ready.

Rollover of each button:

Course 300-A: 3PAO FedRAMP 17020 Requirements: Understanding and Bridging the Gap. This course provides 3PAOs with FedRAMP requirements overlaid on ISO/IEC 17020.

Course 300-B: 3PAO Security Assessment Plan (SAP) Guidance. This course provides 3PAOs with guidance on FedRAMP requirements for creating a robust SAP.

Course 300-C: 3PAO Security Assessment Report (SAR) Guidance. This course provides 3PAOs with guidance on FedRAMP requirements for creating a robust SAR.

Course 300-D: 3PAO Documenting Evidence Procedures. This course provides 3PAOs with guidance on FedRAMP requirements for documenting evidence collected during the assessment and how to populate the SAR.

Course 300-E: 3PAO Vulnerability Scanning Methodology and Documentation. This course provides 3PAOs with guidance on FedRAMP requirements for conducting vulnerability scanning on a system and how the results must be documented to meet FedRAMP requirements for initial authorization assessments and annual assessments.

Course 300-F: Review of Security Assessment Report (SAR) Tables. This course provides 3PAOs with guidance on FedRAMP requirements for populating SAR tables to ensure that all tables are correctly populated.

Course 300-G: Readiness Assessment Report (RAR) Preparation (currently being completed). This course provides a discussion on how the FedRAMP security requirements must align with a CSP’s system security capabilities before the CSP system can be approved as FedRAMP Ready.
300-A (Slide Layer)

300-B (Slide Layer)
300-C (Slide Layer)

FedRAMP 3PAO Readiness Assessment Report (RAR) Preparation

Course 300-C

3PAO Security Assessment Report (RAR) Guidance. This course provides 3PAOs with guidance on FedRAMP requirements for creating a valid SAR.

Here is where you are in your training. Select any of the map points to see where you've been and where you're going.

300-D (Slide Layer)

FedRAMP 3PAO Training Roadmap

Course 300-D

IPA01: Documenting Evidence: Assessment Procedures. This course provides 3PAOs with guidance on FedRAMP requirements for documenting evidence collected during the assessment and how to populate the SAR.

Here is where you are in your training. Select any of the map points to see where you've been and where you're going.
1.4 Course Menu and Learning Objectives

**Notes:**

**Transcript**

**Title**

Course Menu and Learning Objectives

**Text**

Select each item to view the topics and learning objectives

- Intent of the Readiness Assessment Report (RAR)
- RAR Guidelines

---
Today's training will provide an overview of the FedRAMP Readiness Assessment Report and how it works. Select each item to view the topics and learning objectives.

At the end of the course, you will be able to:

- Describe the intent of the Readiness Assessment Report (RAR)
- List RAR Guidelines
- Describe the RAR Level of Effort (LOE)
- List Key FedRAMP Ready Requirements
- Describe RAR Requirements
- Explain the Role of the 3PAO in RAR Development

Readiness Assessment Report (RAR) Intent (Slide Layer)
RAR Guidelines (Slide Layer)

You'll be able to:
- List RAR Guidelines

Select each item to view the topics and learning objectives

RAR Level of Effort (LOE) (Slide Layer)

You'll be able to:
- Describe the RAR Level of Effort (LOE)

Select each item to view the topics and learning objectives
For the FedRAMP 3PAO Readiness Assessment Report (RAR) Preparation:

Key FedRAMP Ready Requirements (Slide Layer)

You'll be able to:
- List Key FedRAMP Ready Requirements

RAR Requirements (Slide Layer)

You'll be able to:
- Describe RAR Requirements
Role of the 3PAO in RAR Development (Slide Layer)

1.5 Intent of the RAR

Notes:

Transcript
Title
Intent of the Readiness Assessment Report (RAR)

Text

Is a CSP Ready for FedRAMP? sliding text

• The intent of the RAR is for both CSPs and the government to understand if a CSP is ready for FedRAMP.
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- CSPs should understand if they have key capabilities to obtain a FedRAMP authorization.
- The FedRAMP PMO should be able to adequately understand if a CSP has a high likelihood of making it through a FedRAMP authorization.

The end result is . . . sliding text

In addition to CSPs being able to ensure they have no major gaps in their system prior to beginning a FedRAMP authorization, approved RARs also provide CSPs with strong evidence of their capabilities to sell to Federal Agencies.

Approved RARs are made available to Federal Agencies through FedRAMP for up to one year after the delivery of a report.

Image
Image of individual using a pen to document a report

Audio
Is a CSP Ready for FedRAMP? This is the essential question to ask. Why?
- The intent of the RAR is for both CSPs and the government to understand if a CSP is ready for FedRAMP.
- CSPs should understand if they have key capabilities to obtain a FedRAMP authorization.
- The FedRAMP PMO should be able to adequately understand if a CSP has a high likelihood of making it through a FedRAMP authorization.
- RARs approved by the FedRAMP PMO signify a CSP is FedRAMP Ready

FedRAMP Ready indicates a CSP has no major gaps in their system prior to beginning a FedRAMP authorization, and provides a CSP with strong evidence of their capabilities to sell to Federal Agencies. Approved RARs are made available to Federal Agencies through FedRAMP for up to one year after delivery.

1.6 RAR Overview (and Guidelines)

Notes:
RAR Overview

Text

RAR Overview on Guidelines

3PAOs Should Focus on Capabilities
- CSPs’ biggest hurdle in obtaining a FedRAMP authorization is the full implementation of capabilities.
- The RAR does NOT require massive evidence gathering by a 3PAO or 100% of the documentation to be completed by a vendor.
- 3PAOs should be focused on understanding how a CSP system works and operates, NOT on how that is translated to documentation.

3PAOs Should Validate What’s Implemented, Not What’s Written
- Technical writing is difficult and many times not accurate.
- FedRAMP requires 3PAOs to validate what’s implemented in the CSP system and not reiterate what a CSP has written.
- Stated another way, a 3PAO must validate in the RAR what the CSP system is and what it isn’t.

Not All CSPs Will Pass the RAR
- 3PAOs should tell their CSPs that a Readiness Assessment is intended to determine readiness, not guarantee it.
- Many times a readiness assessment will find significant gaps in CSP capabilities, resulting in the identification of work for a CSP.
- FedRAMP grants a FedRAMP Ready designation when the information in the RAR indicates that the CSP is likely to achieve a Joint Authorization Board (JAB) Provisional Authorization-to-Operate (P-ATO) or Agency ATO for the system.
- 3PAOs should NOT submit a RAR to FedRAMP unless they believe a CSP has all of the necessary capabilities to obtain a FedRAMP authorization.

Image

Image of chairs in a conference room

Audio

Let’s continue with our discussion on the guidelines of the RAR. Specifically, let’s explore three key areas:

Button 1: 3PAOs Should Focus on Capabilities. CSPs’ biggest hurdle in obtaining a FedRAMP authorization is the full implementation of capabilities. It’s important to recognize that the RAR does NOT require massive evidence gathering by a 3PAO or 100% of the documentation to be completed by a vendor. Ultimately, 3PAOs should be focused on understanding how a CSP system works and operates, not on how that is translated to documentation.

Button 2: 3PAOs Should Validate What’s Implemented, Not What’s Written. Technical writing is difficult and many times not accurate. FedRAMP requires 3PAOs to validate what’s implemented in a CSP system and NOT reiterate what a CSP has written. So, in other words, a 3PAO must validate in the RAR what the CSP system is and what it’s not.

Button 3: Not All CSPs Will Pass the RAR: 3PAOs should tell their CSPs that a Readiness Assessment is intended to determine readiness, not guarantee it. We find that, on many occasions, a Readiness Assessment will identify significant gaps in CSP capabilities, which results in the identification of work for a CSP. FedRAMP grants a FedRAMP Ready designation when the information in the RAR indicates that the CSP is likely to achieve a Joint Authorization Board (JAB) Provisional Authorization-to-Operate (P-ATO) or Agency ATO for the system. 3PAOs must NOT submit a RAR to FedRAMP unless they believe a CSP has all of the necessary
capabilities to obtain a FedRAMP authorization.

**Bullet 1 (Slide Layer)**

- SPAOs Should Focus on Capabilities
  - CSP’s biggest hurdle in obtaining a FedRAMP authorization is the full implementation of capabilities.
  - The RAR does NOT require massive evidence gathering by a 3PAO or 32% of the documentation to be completed by a vendor.
  - SPAOs should be focused on understanding how a CSP system works and operates, NOT on how that is translated to documentation.

**Bullet 2 (Slide Layer)**

- SPAOs Should Validate What’s Implemented, Not What’s Written
  - Technical writing is difficult and many times not accurate.
  - FedRAMP requires 3PAOs to validate what’s implemented in the CSP system and not reiterate what a CSP has written.
  - Stated another way, a 3PAO must validate in the RAR what the CSP system is and what it isn’t.
Bullet 3 (Slide Layer)

1.7 Knowledge Check

(True/False, 10 points, 1 attempt permitted)

<table>
<thead>
<tr>
<th>Correct Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>False</td>
</tr>
</tbody>
</table>

Feedback when correct:
That's right! You selected the correct response. The answer is False as you learned that the RAR does NOT require massive evidence gathering by a 3PAO or 100% of the documentation to be completed by a CSP. Furthermore, 3PAOs should be focused on understanding how a CSP system works and operates, not on how that is translated to documentation.

Feedback when incorrect:

Sorry! You should have known that the RAR does NOT require massive evidence gathering by a 3PAO or 100% of the documentation to be completed by a CSP. Furthermore, 3PAOs should be focused on understanding how a CSP system works and operates, not on how that is translated to documentation.
Incorrect (Slide Layer)

Try Again (Slide Layer)
1.8 RAR Level of Effort

Notes:

Transcript
Title
RAR Level of Effort

Text
Estimated 2-4 Week Completion Time

- In the creation of the Readiness Assessment, FedRAMP worked with 3PAOs to estimate what would be sufficient to do a thorough assessment and write a quality report without making the cost too high for vendors.

- The PMO estimates that a Readiness Assessment should take anywhere from 1-2 weeks to complete as well as 1-2 weeks to compile the report (for an average system).

- 3PAO notifies FedRAMP PMO of RAR via info@fedramp.com >mailto:info@fedramp.com< within 2 weeks of submission.

- High RARS are handled differently from Moderate RARs.

Variability Based on Size, Complexity, Cooperation, and Preparedness of CSP

- This is not to say that all CSPs for a Readiness Assessment will take 2-4 weeks to complete.

- CSPs must be prepared for the assessment (right staff available; provide evidence, reports, etc. to the 3PAO).

- Additionally, the size and complexity of a CSP will factor heavily into the level of effort.

Audio
Let’s discuss a very important element of RAR preparation, namely the level of effort.

A 2-4 Week RAR completion time is an estimate. In the creation of the Readiness Assessment, FedRAMP worked with 3PAOs to estimate what would be sufficient to do a thorough assessment and write a quality report without making the cost too high for vendors. The PMO estimates that a Readiness Assessment should take anywhere from 1-2 weeks to complete as well as 1-2 weeks
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

to compile the report (for an average system). 3PAO notifies FedRAMP PMO of RAR via info@fedramp.com within 2 weeks of submission. High RARS are handled differently from Moderate RARs.

Be mindful that the 2 - 4 Week completion time is based on size, complexity, cooperation, and preparedness of the CSP. In other words, this is not to say that all CSP Readiness Assessments will take 2-4 weeks to complete. CSPs must be prepared for the assessment (right staff available; provide evidence, reports, etc. to the 3PAO). Additionally, the size and complexity of a CSP will factor heavily into the level of effort.

1.9 Key FedRAMP Ready Requirements

Notes:

Transcript

Title

Key FedRAMP Ready Requirements

Text

The seven key FedRAMP Ready requirements that must be sufficiently documented in the RAR include (select each button to reveal each requirement):

- 3PAO Attestation
- Federal Mandates
- Accurate Boundary
- In-Person Discussions
- Adequate Segregation
- Timely Vulnerability Remediation
- Proof of SSP Documentation
Now, let's begin a review of the seven key FedRAMP Ready requirements. These requirements include the following:

- 3PAO Attestation
- Federal Mandates
- Accurate Boundary
- In-Person Discussions
- Adequate Segregation
- Timely Vulnerability Remediation
- Proof of SSP Documentation
Bullet 2 (Slide Layer)

- Federal Mandates

Bullet 3 (Slide Layer)

- Accurate Boundary
Bullet 4 (Slide Layer)

- In-Person Discussions

Bullet 5 (Slide Layer)

- Adequate Segregation
1.10 Key FedRAMP Ready Requirements--3PAO Attestation

Notes:

Transcript

Title

Key FedRAMP Ready Requirement: 3PAO Attestation

Text

It’s important that you learn and understand the seven key FedRAMP Ready Requirements.

Let’s begin with 3PAO Attestation. An accredited 3PAO must attest to CSP Readiness, in writing.

• 3PAOs must use “expert judgment to subjectively evaluate a CSP’s overall readiness and factor this evaluation into their attestation.”

• 3PAOs must perform a full authorization boundary validation by
  • Ensuring nothing is missing from the CSP-identified boundary
  • Ensuring all included items are actually present and part of the system inventory.

• 3PAOs must perform activities including, but not limited to, discovery scans, in-person interviews, and physical inspections. 3PAOs must describe all leveraged services (authorized and unauthorized).

• 3PAOs must describe how a CSP scans operating system (OS)/infrastructure, web applications (Web Apps), and Databases

Image

Image of laptop computer bag

Audio

Let’s begin with the 3PAO attestation. An accredited 3PAO must attest to a CSP’s readiness in writing. This is accomplished by the following:
1. 3PAOs must use “expert judgment to subjectively evaluate a CSP’s overall readiness and factor this evaluation into their attestation.”

2. 3PAOs must perform a full authorization boundary validation by
   - Ensuring nothing is missing from the CSP-identified boundary
   - Ensuring all included items are actually present and part of the system inventory

3. 3PAOs must perform activities including, but not limited to, discovery scans, in-person interviews, and physical inspections.

4. 3PAOs must describe all leveraged services (authorized and unauthorized).

Bullet 1 (Slide Layer)

Bullet 2 (Slide Layer)
Bullet 3 (Slide Layer)

3PAOs must perform activities including, but not limited to, discovery scans, in-person interviews, and physical inspections. 3PAOs must describe all leveraged services (authorized and unauthorized).

Bullet 4 (Slide Layer)

3PAOs must describe how a CSP scans operating system (OS)/infrastructure, web applications (Web Apps), and databases.
1.11 Key FedRAMP Ready Requirements--Federal Mandates

Notes:

Transcript

Title

Key FedRAMP Ready Requirement: Federal Mandates

Text

It’s important that you learn and understand the seven key FedRAMP Ready requirements.

Let’s continue with Federal Mandates. An accredited 3PAO must attest to a CSP’s compliance with the following federal mandates:

- FIPS 140-2 Validated or National Security Agency (NSA)-approved cryptographic modules consistently used within the system
- System supports user authentication via agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials
- System operates at the minimum eAuth level for its FIPS-199 level of operation (Level 3 for Moderate and Level 4 for High impact systems)
- CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements

Image

Image of shaded White House

Audio

With respect to Federal Mandates, an accredited 3PAO must attest to a CSP’s compliance with the following federal mandates:

1. FIPS 140-2 Validated or National Security Agency (NSA)-approved cryptographic modules consistently used within the system
2. System supports user authentication via agency Common Access Card (CAC) or Personal Identity Verification (PIV) credentials
3. System operates at the minimum eAuth level for its FIPS-199 level of operation (Level 3 for Moderate and Level 4 for High impact systems)

4. CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements

**Bullet 1 (Slide Layer)**

Select each button to view more information

**Bullet 2 (Slide Layer)**

Select each button to view more information
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

Bullet 3 (Slide Layer)

System operates at the minimum eAuth level for its FIPS-199 level of operation (Level 3 for Moderate and Level 4 for High impact systems)

1 2 3 4

Select each button to view more information

Bullet 4 (Slide Layer)

CSP and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements

1 2 3 4

Select each button to view more information
1.12 Key FedRAMP Ready Requirements--Accurate Boundary

Notes:

Transcript
Title
Key FedRAMP Ready Requirement: Accurate Boundary

Text
Let's proceed with accurate boundary. It's IMPORTANT to understand that ensuring the authorization boundary is accurate in the RAR is critical to FedRAMP authorization activities. Boundary inaccuracies within the RAR may give authorizing officials and FedRAMP grounds for removing a vendor from assessment and authorization activities.

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:

- Conducting a discovery scan as part of a Readiness Assessment.
  - A discovery scan is intended to provide a technical ability to ensure that things like all virtual LANS (VLANS), subnets, and undocumented hosts are discovered, logical, and provide adequate security.
- Analyzing all border devices to ensure they provide appropriate segregation from other systems.
  - This analysis includes examinations of all device configurations including network configurations.
- Describing all leveraged services (authorized and unauthorized).
- Describing how a CSP scans OS/infrastructure, web apps, and databases.
- Ensuring the boundary makes sense - just because a boundary is accurate doesn't mean it always provides adequate security.

Image
Image of laptop computer and a paper notepad with pen

Audio
Let’s proceed with accurate boundary. It’s IMPORTANT to understand that ensuring the authorization boundary is accurate in the RAR is critical to FedRAMP authorization activities. Boundary inaccuracies within the RAR may give authorizing officials and FedRAMP grounds for removing a vendor from assessment and authorization activities. Here’s what needs to occur with this requirement:

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:

- Conducting a discovery scan as part of a Readiness Assessment.
  - A discovery scan is intended to provide a technical ability to ensure that things like all virtual LANS (VLANS), subnets, and undocumented hosts are discovered, logical, and provide adequate security.
- Analyzing all border devices to ensure they provide appropriate segregation from other systems.
  - This analysis includes examinations of all device configurations including network configurations.
- Describing all leveraged services (authorized and unauthorized).
- Describing how a CSP scans OS/infrastructure, web apps, and databases.
- Ensuring the boundary makes sense - just because a boundary is accurate doesn’t mean it always provides adequate security.
Bullet 2 (Slide Layer)

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:

- Analyzing all border devices to ensure they provide appropriate segregation from other systems.
  - This analysis includes examinations of all device configurations including network configurations.

1 2 3 4 5

Select each button to view more information

Bullet 3 (Slide Layer)

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:

- Describing all leveraged services (authorized and unauthorized).

1 2 3 4 5

Select each button to view more information
Bullet 4 (Slide Layer)

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:
- Describing how a CSP scans OS/infrastructure, web apps, and databases.

Bullet 5 (Slide Layer)

3PAOs must validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary by:
- Ensuring the boundary makes sense - just because a boundary is accurate doesn’t mean it always provides adequate security.

1.13 Knowledge Check

(Multiple Choice, 10 points, 2 attempts permitted)
Correct Choice

<table>
<thead>
<tr>
<th>Correct Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate Boundary</td>
</tr>
<tr>
<td>Attestation</td>
</tr>
<tr>
<td>X</td>
</tr>
<tr>
<td>Federal Mandates</td>
</tr>
<tr>
<td>In-Person Discussion</td>
</tr>
</tbody>
</table>

**Feedback when correct:**

That's right! You selected the correct response. The requirement that addresses how a system operates at the minimum eAuth level for its FIPS-199 level of operation (Level 3 for Moderate and Level 4 for High impact systems) is a Federal Mandate.

**Feedback when incorrect:**

Sorry! You should have known that the requirement that addresses how a system operates at the minimum eAuth level for its FIPS-199 level of operation (Level 3 for Moderate and Level 4 for High impact systems) is a Federal Mandate.
Correct (Slide Layer)

Incorrect (Slide Layer)
1.14 Key FedRAMP Ready Requirements--In-Person Discussions

Let's continue with In-Person Discussions, which is our fourth key FedRAMP ready requirement.

Notes:

Transcript

Title

Key FedRAMP Ready Requirement: In-Person Discussions

Text

Let's continue with In-Person Discussions, which is our fourth key FedRAMP ready requirement.
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- All Readiness Assessments must include some portion of in-person interviews and observations. This means a 3PAO must, in person, examine a CSP's organizational maturity and operations in action. This is not something that can be completed over video chats or over the phone.

- While in-person data center visits are not mandatory, a 3PAO must be able to adequately state that data centers are not a major concern if they are the responsibility of a CSP.

**Image**

A series of images of a man standing on the right side of the screen, talking about the two examples on the screen.

**Audio**

Let's continue with In-Person Discussions, which is our fourth key FedRAMP ready requirement. All Readiness Assessments must include some portion of in-person interviews and observations. This means a 3PAO must, in person, examine a CSP’s organizational maturity and operations in action. This is not something that can be completed over video chats or over the phone. While in-person data center visits are not mandatory, a 3PAO must be able to adequately state that data centers are not a major concern if they are the responsibility of a CSP.

### 1.15 Knowledge Check

*(True/False, 10 points, 1 attempt permitted)*

<table>
<thead>
<tr>
<th>Correct Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
</tr>
<tr>
<td>X False</td>
</tr>
</tbody>
</table>
Feedback when correct:

That’s right! You selected the correct response. The answer is False. Data center visits are NOT mandatory, but a 3PAO must be able to adequately state that data centers are not of a major concern if they are the responsibility of a CSP.

Feedback when incorrect:

Sorry! You should have known that data center visits are NOT mandatory, but a 3PAO must be able to adequately state that data centers are not of a major concern if they are the responsibility of a CSP.

Correct (Slide Layer)
Incorrect (Slide Layer)

![Incorrect Knowledge Check](image)

Try Again (Slide Layer)

![Try Again Knowledge Check](image)
1.16 Key FedRAMP Ready Requirements--Adequate Segregation

Notes:

Transcript
Title
Key FedRAMP Ready Requirement: Adequate Segregation

Text
Let's continue with Adequate Segregation. It's critical that

- CSPs provide proof to their 3PAO to validate adequate segregation of tenants (where a common architecture and code base is centrally maintained) and data.
- 3PAOs analyze a prior penetration test - even if completed by the CSP or another assessor.
  - More importantly, complete a penetration test, but it’s not an explicit requirement for a Readiness Assessment.
  - If a CSP has not had a penetration test, the 3PAO must be able to provide rationale for proving there is adequate segregation of tenants and data. The 3PAO must base the 3PAO validated assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved.

Image
Image of backdrop of a computer monitor

Audio
Let's continue with Adequate Segregation. It’s critical that

- CSPs provide proof to their 3PAO to validate adequate segregation of tenants (where a common architecture and code base is centrally maintained) and data.
- 3PAOs analyze a prior penetration test - even if completed by the CSP or another assessor.
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- It is a best practice and an ultimate requirement of FedRAMP to complete a penetration test, but it’s not an explicit requirement for a Readiness Assessment.
- If a CSP has not had a penetration test, the 3PAO must be able to provide rationale for proving there is adequate segregation of tenants and data. The 3PAO must base the 3PAO validated assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved.

Panel 1 (Slide Layer)

Panel 2 (Slide Layer)
Panel 3 (Slide Layer)

1.17 Key FedRAMP Ready Requirements--Timely Vulnerability Remediation

Notes:

Transcript
Title
Key FedRAMP Ready Requirement: Timely Vulnerability Remediation

Text
Let’s continue with Timely Vulnerability Remediation. It’s critical that:
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- The FedRAMP requirements for remediation of risks are clearly being followed
  - CSPs have 30 days to remediate High vulnerabilities.
  - CSPs have 90 days to remediate Moderate vulnerabilities.
- 3PAOs identify that a CSP has an established risk management strategy that includes remediating vulnerabilities in a timely manner.
- CSPs understand that they do not have to track vulnerabilities in the exact FedRAMP format (Plan of Actions and Milestones (POA&M) template), but the vulnerabilities must be tracked.
- CSPs provide their 3PAO with evidence of a demonstrated capability to manage risk and remediate vulnerabilities in a timely manner.

Image
Image of backdrop of a computer keyboard

Audio
Let’s continue with Timely Vulnerability Remediation. It’s critical that:

- The FedRAMP requirements for remediation of risks are clearly being followed
  - CSPs have 30 days to remediate High vulnerabilities.
  - CSPs have 90 days to remediate Moderate vulnerabilities.
- 3PAOs identify that a CSP has an established risk management strategy that includes remediating vulnerabilities in a timely manner.
- CSPs understand that they do not have to track vulnerabilities in the exact FedRAMP format (Plan of Actions and Milestones (POA&M) template), but the vulnerabilities must be tracked.
- CSPs provide their 3PAO with evidence of a demonstrated capability to manage risk and remediate vulnerabilities in a timely manner.

Bullet 1 (Slide Layer)
Bullet 2 (Slide Layer)

3PAOs identify that a CSP has an established risk management strategy that includes remediating vulnerabilities in a timely manner.

Bullet 3 (Slide Layer)

CSPs understand that they do not have to track vulnerabilities in the exact FedRAMP format (Plan of Actions and Milestones (POA&M) template), but the vulnerabilities must be tracked.
1.18 Key FedRAMP Ready Requirement: System Security Plan (SSP) Documentation

Let's conclude with System Security Plan (SSP) Documentation. For a Readiness Assessment, it’s important to know that:
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- CSPs' FedRAMP required documentation does not have to be 100% complete.
- The intent of the RAR is to determine the capabilities of a CSP, not to review the documentation of a CSP.
- 3PAOs must focus on reviewing CSP capabilities/functionality and understanding the system operations of a CSP.
- CSPs must provide documentation that includes policies, procedures, and internal guidance, to prove their organizational maturity.
- If a CSP has not begun documenting an SSP, and has not completed a majority of the document, it would be difficult to prove “FedRAMP Readiness”

Image
Image of three individuals pointing out an important area on a sheet of paper

Audio
Let’s conclude with System Security Plan (SSP) Documentation. For a Readiness Assessment, it’s important to know that:

- CSPs’ FedRAMP required documentation does not have to be 100% complete.
- The intent of the RAR is to determine the capabilities of a CSP, not to review the documentation of a CSP.
- 3PAOs must focus on reviewing CSP capabilities/functionality and understanding the system operations of a CSP.
- CSPs must provide documentation that includes policies, procedures, and internal guidance, to prove their organizational maturity.
- If a CSP has not begun documenting an SSP, and has not completed a majority of the document, it would be difficult to prove “FedRAMP Readiness”

Bullet 1 (Slide Layer)
Bullet 2 (Slide Layer)

The intent of a Readiness Capability is to determine the capabilities of a CSP, not to review the documentation of a CSP.

Bullet 3 (Slide Layer)

3PAOs must focus on reviewing CSP capabilities/functionality and understanding the system operations of a CSP.
Bullet 4 (Slide Layer)

CSPs must provide documentation that includes policies, procedures, and internal guidance, to prove their organizational maturity.

1 2 3 4 5
Select each button to view more information

Bullet 5 (Slide Layer)

If a CSP has not begun documenting an SSP, and has not completed a majority of the document, it would be difficult to prove "FedRAMP Readiness".

1 2 3 4 5
Select each button to view more information
1.19 FedRAMP Readiness Assessment Report Requirements

Notes:

Transcript
Title
FedRAMP RAR Requirements

Image
Image of FedRAMP RAR Requirements in a slider framework with the backdrop of a laptop computer

Text
At a minimum, 3PAOs must consider the following when evaluating a CSP’s overall “FedRAMP Readiness” as outlined in the RAR Executive Summary:

- Requirement #1: The CSP must have an overall alignment with the National Institute of Standards and Technology (NIST) definition of cloud computing according to NIST SP 800-145
- Requirement #2: The 3PAO must assess the CSP’s notable strengths and weaknesses
- Requirement #3: The CSP must prove to the 3PAO that they have the ability to consistently maintain a clearly defined system boundary
- Requirement #4: The CSP must prove to the 3PAO that they have clearly defined customer responsibilities
- Requirement #5: The CSP must prove to the 3PAO that all unique or alternative implementations have been accounted
- Requirement #6: The CSP must prove to the 3PAO that the overall maturity level relative to the system type, size, and complexity

Audio
At a minimum, the 3PAOs must consider the following when evaluating a CSP’s overall “FedRAMP Readiness” as outlined in the RAR Executive Summary:

- Requirement #1: The CSP must have an overall alignment with the National Institute of Standards and Technology (NIST) definition of cloud computing according to NIST SP 800-145
• Requirement  #2: The 3PAO must assess the CSP’s notable strengths and weaknesses
• Requirement  #3: The CSP must prove to the 3PAO that they have the ability to consistently maintain a clearly defined system boundary
• Requirement  #4: The CSP must prove to the 3PAO that they have clearly defined customer responsibilities
• Requirement  #5: The CSP must prove to the 3PAO that all unique or alternative implementations have been accounted
• Requirement  #6: The CSP must prove to the 3PAO that the overall maturity level relative to the system type, size, and complexity

1 (Slide Layer)
Alignment with NIST SP 800-145 link

RAR Requirement Step #1: Alignment with NIST SP 800-145

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 Definition of Cloud Computing, September 2011

- On-demand self-service - user unilaterally provisions computing capabilities automatically
- Broad network access - availability over the network and accessed through standard mechanisms
- Resource pooling - CSP compute resources pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand
- Rapid elasticity - capabilities elastically provisioned and released automatically, to meet demand
- Measured service - CSPs automatically control and optimize resource use by leveraging a metering capability

Notes:

Transcript
Title
RAR Requirement: Step #1: Alignment with NIST SP 800-145

Text
The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 Definition of Cloud Computing, September 2011

- On-demand self-service - user unilaterally provisions computing capabilities automatically
- Broad network access - availability over the network and accessed through standard mechanisms
- Resource pooling - CSP compute resources pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand
- Rapid elasticity - capabilities elastically provisioned and released automatically, to meet demand
- Measured service - CSPs automatically control and optimize resource use by leveraging a metering capability

Image
Image of man speaking about a particular topic

Audio
With the FedRAMP RAR Requirement: Step #1: Alignment with NIST SP 800-145, there are five CSP attributes that a 3PAO must assess:

- Does the CSP provide on-demand self-service, which means the user unilaterally provisions computing capabilities automatically?
- Does the CSP provide broad network access, whereby there is availability over the network and accessed through standard
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

mechanisms?

• Does the CSP provide resource pooling where a CSP compute resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand?

• Does the CSP provide rapid elasticity which means that capabilities are elastically provisioned and released automatically, to meet demand?

• Is this a measured service where CSPs automatically control and optimize resource use by leveraging a metering capability?

2 (Slide Layer)

Notable strengths and weaknesses link

RAR Requirement Step #2: Notable Strengths and Weaknesses

Notes:
Title
RAR Requirement: Step #2: Notable strengths and weaknesses

Text
Notable strengths and weaknesses

• CSPs should understand if they have key capabilities, which include the notable strengths to be able to obtain a FedRAMP authorization.

• 3PAOs should be able to identify CSP Cloud Service Offering weaknesses through the Readiness Assessment process.

• By the conclusion of the Readiness Assessment, the FedRAMP PMO should be able to adequately understand if a CSP’s Cloud Service Offering has a high likelihood of making it through a FedRAMP authorization.

Audio
With respect to FedRAMP RAR Requirement: Step #2, the CSP must exhibit notable strengths and weaknesses. CSPs should understand fully if they have key capabilities, which include notable strengths to be able to obtain a FedRAMP authorization.

Ultimately, 3PAOs should be able to identify CSP Cloud Service Offering weaknesses through the Readiness Assessment process.

By the conclusion of a Readiness Assessment, the FedRAMP PMO should be able to adequately understand if a CSP’s Cloud Service Offering has a high likelihood of making it through a FedRAMP authorization.
Ability to consistently maintain a clearly defined system boundary link

RAR Requirement Step #3: Ability to consistently maintain a clearly defined system boundary

Notes:

Transcript
Ability to Consistently Maintain a Clearly Defined System Boundary:

- Resource pooling and rapid elasticity are provisioned in such a way that the overall integrity of the system boundary is maintained.
- 3PAOs validate that the boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary.
- 3PAOs ensure that the boundary makes sense physically and logically, and provides adequate security.
- 3PAOs perform a discovery scan as part of a Readiness Assessment, intended to provide a technical ability to ensure that things like all VLANS, subnets, and undocumented hosts discovered.
- 3PAOs analyze all border devices to ensure these provide appropriate segregation from any other systems that include examinations of all configurations to analyze network configurations.

Audio

Regarding FedRAMP RAR Requirement: Step #3, CSPs must be able to consistently maintain a clearly defined system boundary. This means 3PAOs must:

- Validate that the Cloud Service Offering has resource pooling and rapid elasticity that are provisioned in such a way that the overall integrity of the system boundary is maintained.
- Validate that the CSP Cloud Service Offering boundary is accurate - identifying BOTH what is inside the boundary AND outside the boundary.
- Ensure that the CSP boundary makes sense physically and logically, and provides adequate security.
- Perform a discovery scan, intended to provide a technical ability to ensure that things like all VLANS, subnets, undocumented hosts, are discovered.
- Analyze all border devices to ensure these provide appropriate segregation from any other systems that include examinations of all configurations to analyze network configurations.
Clearly defined customer responsibilities link

**RAR Requirement Step #4: Clearly defined customer responsibilities**

Notes:

Transcript
Title
RAR Requirement: Step #4, Clearly Defined Customer Responsibilities

Image
Clearly defined customer responsibilities involve:
• Clarity and consistency in security control implementations details.
• A System Security Plan (SSP) writer who accurately determines how the customer responsibility requirement is portrayed for one security control implementation detail and uses the same format throughout the SSP for each control that has a customer responsibility requirement.
• Customer responsibilities that are unambiguous and clearly described and NOT how the customer implements the requirement (it’s the customer responsibility to define how the control is implemented in their leveraging environment).
• Ensuring all customer requirements in the SSP MATCH the customer requirements in the FedRAMP Control Implementation Summary (CIS) and in the Customer Responsibility Matrix (CRM).

Audio
As you encounter FedRAMP Readiness Assessment Report Requirement: Step #4, there are four defined customer responsibilities. This involves the following:
• Clarity and consistency in security control implementations details.
• A System Security Plan (SSP) writer who accurately determines how the customer responsibility requirement is portrayed for one security control implementation detail and uses the same format throughout the SSP for each control that has a customer responsibility requirement.
• Customer responsibilities that are unambiguous and clearly described and NOT how the customer implements the requirement (it’s the customer responsibility to define how the control is implemented in their leveraging environment).
• Ensuring all customer requirements in the SSP MATCH the customer requirements in the FedRAMP Control Implementation Summary (CIS) and in the Customer Responsibility Matrix (CRM).
RAR Requirement Step #5: Unique or Alternative Implementations

3PAOs should ensure that any unique or alternative implementations are:

- Consistent with the intent of the security control and principles articulated within the security control implementation in the CSP environment.
- Recognizing and acknowledging unique security control implementations that meet the intent of the security control.
- Recognizing and acknowledging the alternative implementation of a security control implementation that still meets the intent of the security control.
- It is the responsibility of the CSP to clearly define and be knowledgeable concerning all unique and alternative security control implementations within the Cloud Service Offering.

Notes:

Transcript
Title
RAR Requirement: Step #5, Unique or Alternative Implementations
3PAOs should assess unique or alternative implementations by:

- Considering the intent of the security concepts and principles articulated within the security control as implemented in the CSP environment.
- Recognizing and acknowledging unique security controls implementations that meet the intent of the security control.
- Recognizing and acknowledging the alternative implementation of a security control implementation that still meets the intent of the security control.
- It is the responsibility of the CSP to clearly define and be knowledgeable concerning all unique and alternative security control implementations within the Cloud Service Offering.

Audio

In Step #5, the FedRAMP RAR Requirement refers to how 3PAOs should assess unique or alternative implementations. This involves the 3PAO to:

- Considering the intent of the security concepts and principles articulated within the security control as implemented in the CSP environment.
- Recognizing and acknowledging unique security controls implementations that meet the intent of the security control.
- Recognizing and acknowledging the alternative implementation of a security control implementation that still meets the intent of the security control.
- It is the responsibility of the CSP to clearly define and be knowledgeable concerning all unique and alternative security control implementations within the Cloud Service Offering.
Overall maturity level relative to the system type, size, and complexity link

RAR Requirement Step #6, Overall Maturity Level Relative to the System Type, Size, and Complexity

Notes:

Transcript
Title
RAR Requirement: Step #6, Overall Maturity Level Relative to the System Type, Size, and Complexity

Image
Image of NIST SP 800 53-A

Text
Overall maturity level relative to the system type, size, and complexity centers on:

- CSPs having documented processes, procedures, and having significant progress towards completed documentation.
- FedRAMP understanding if a CSP has mature operations to maintain a low level of risk.
- 3PAOs updating their RAR to identify:
  - Staffing levels to ensure CSP have adequate resources to provide continued implementation of security controls.
  - Change management maturity - to ensure CSPs have a mature process for introducing changes to their environment.
  - Continuous monitoring capabilities - to ensure CSPs have an ability to appropriately manage the risk in their environment.

Audio
The overall maturity level relative to the system type, size, and complexity centers on:

- CSPs having documented processes, procedures, and having significant progress towards completed documentation.
- FedRAMP understanding if a CSP has mature operations to maintain a low level of risk.
- 3PAOs updating their RAR to identify:
  - Staffing levels to ensure CSP have adequate resources to provide continued implementation of security controls.
  - Change management maturity - to ensure CSPs have a mature process for introducing changes to their environment.
  - Continuous monitoring capabilities - to ensure CSPs have an ability to appropriately manage the risk in their environment.

1.20 Knowledge Check

(Multiple Choice, 10 points, 2 attempts permitted)
Correct Choice

<table>
<thead>
<tr>
<th>Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate Boundary</td>
</tr>
<tr>
<td>X Adequate Segregation</td>
</tr>
<tr>
<td>SSP Documentation</td>
</tr>
<tr>
<td>Timely Vulnerability Remediation</td>
</tr>
</tbody>
</table>

**Feedback when correct:**

That's right! You selected the correct response. Adequate Segregation is the specific requirement that addresses when FedRAMP recommends that a Penetration Test be reviewed - even if completed by the CSP or another assessor.

**Feedback when incorrect:**

Incorrect! You should have known that Adequate Segregation is the specific requirement that addresses when FedRAMP recommends that a Penetration Test be reviewed - even if completed by the CSP or another assessor.
Correct (Slide Layer)

Incorrect (Slide Layer)
1.21 The Role of the 3PAO in RAR Development

Notes:

Transcript
Title
The Role of the 3PAO in RAR Development

Text
The Role of the 3PAO in RAR Development
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

Select each button to view more information.

- **Button 1: Option #1: 3PAO Consults;**
  - CSPs' biggest hurdle in obtaining a FedRAMP authorization is the full implementation of capabilities.
    - The 3PAO may consult with the CSP and assist them in implementing security in the system
    - The 3PAO may provide consulting services to the CSP to write the SSP
    - This same 3PAO MAY NOT test the system for FedRAMP Readiness
    - This does not mean the CSP is FedRAMP Ready. A FedRAMP Readiness Assessment must still be done.

- **Button 2: Option #2: 3PAO FedRAMP Readiness Assessment. Two activities occur:**
  - CSP not ready (and the 3PAO consults). The same 3PAO may assist the CSP to become FedRAMP Ready; the same 3PAO may NOT perform another FedRAMP Readiness Assessment on this CSP; OR
    - The first 3PAO assists the CSP to become FedRAMP Ready
      - A different 3PAO may now perform the second FedRAMP Readiness Assessment
      - The CSP may then become certified as FedRAMP Ready
  - Button 3: Option #3: The same 3PAO must not perform consulting services for the same CSP between FedRAMP Readiness Assessments

**Image**

Image of three buttons in the selection of the big picture of the Role of the 3PAO in RAR Development

**Audio**

Let's continue with our discussion on the Role of the 3PAO in RAR Development. Specifically, let's explore three key options:

- **Option #1: 3PAO Consults:**
  - CSPs' biggest hurdle in obtaining a FedRAMP authorization is the full implementation of capabilities.
    - The 3PAO may consult with the CSP and assist them in implementing security in the system
    - The 3PAO may provide consulting services to the CSP to write the SSP
    - This same 3PAO MAY NOT test the system for FedRAMP Readiness
    - This does not mean the CSP is FedRAMP Ready. A FedRAMP Readiness Assessment must still be done.

- **Option #2: 3PAO FedRAMP Readiness Assessment. Two activities occur:**
  - CSP not ready (and the 3PAO consults). The same 3PAO may assist the CSP to become FedRAMP Ready; the same 3PAO may NOT perform another FedRAMP Readiness Assessment on this CSP; OR
    - The first 3PAO assists the CSP to become FedRAMP Ready
      - A different 3PAO may now perform the second FedRAMP Readiness Assessment
      - The CSP may then become certified as FedRAMP Ready

- **Option #3: 3PAO May Not Consult and Assess the Same System**
  - The same 3PAO must not perform consulting services for the same CSP between FedRAMP Readiness Assessments
    - 3PAOs, NOT CSPs, should upload RARs; this is to ensure chain of custody
    - 3PAOs should not provide RARs without approval from a CSP
    - 3PAOs must only submit RARs if they believe a CSP meets the required capabilities
Be sure to select the Resources link (located in the upper right hand corner of the screen) to download a reference guide to the RAR Development process.

**Button 1 (Slide Layer)**

![Diagram of Role of 3PAO in RAR Development: Option 1](image1)

**Button 2 (Slide Layer)**

![Diagram of Role of 3PAO in RAR Development: Option 2](image2)
1.22 Summary

The key points that you learned are:

- The Significance of the Readiness Assessment Report (RAR) is that it provides FedRAMP with a sound basis that the CSP will be capable of proceeding with the FedRAMP process and should have success in doing so.
FedRAMP Training - 3PAO Readiness Assessment Report (RAR) Preparation

- Key FedRAMP Ready Requirements provide a high level view of the 3PAO expertise required in order that the 3PAO can confidently attest to the FedRAMP Readiness of a CSP.
- FedRAMP Readiness Report Requirements illustrate what specifically must be included in the RAR in order to be acceptable for FedRAMP.

Audio
We have come to the conclusion of this course. The key points that you learned are:

- The Significance of the Readiness Assessment Report (RAR) is that it provides FedRAMP with a sound basis that the CSP will be capable of proceeding with the FedRAMP process and should have success in doing so.
- Key FedRAMP Ready Requirements provide a high level view of the 3PAO expertise required in order that the 3PAO can confidently attest to the FedRAMP Readiness of a CSP.
- Finally, FedRAMP Readiness Report Requirements illustrate what specifically must be included in the RAR in order to be acceptable for FedRAMP Readiness Report Requirements illustrates what specifically must be included in the RAR in order to be acceptable for FedRAMP.

1.23 What's Next?

Notes:

Transcript
Title
What’s Next?

Image
Image of FedRAMP logo with a laptop computer
Audio
Select Exit to leave the course and take the 3PAO Readiness Assessment Report Exam. You’ve now completed this course and are now eligible to enroll in other available courses. Please visit the GSA Blackboard Learn Portal for more information or send us an email at info@fedramp.gov <mailto:info@fedramp.gov>.

Text
For more information, please contact us or visit us at any of the following websites:
http://FedRAMP.gov
http://gsa.gov/FedRAMP
@FederalCloud

References
- Penetration Guidance
- NIST 800 53
- A2LA Website
- SAP Template
- Rev 4 Test Case Workbook